

- [12] T. Johansson and E. Pasalic, "A construction of resilient functions with high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 494–501, Feb. 2003.
- [13] K. Kurosawa, T. Satoh, and K. Yamamoto, "Highly nonlinear  $t$ -resilient functions," *J. Universal Comput. Sci.*, vol. 3, no. 6, pp. 721–729, 1997.
- [14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
- [15] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology—EUROCRYPT 1991 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, pp. 378–386.
- [16] —, "Differentially uniform mapping for cryptography," in *Advances in Cryptology—EUROCRYPT 1993 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, pp. 55–65.
- [17] E. Pasalic and S. Maitra, "Linear codes in generalized construction of resilient functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2182–2191, Aug. 2002.
- [18] B. Preneel, "Analysis and design of cryptographic hash functions," Ph.D. dissertation, K.U. Leuven, 1993.
- [19] O. S. Rothaus, "On bent functions," *J. Comb. Theory*, ser. A, vol. 20, pp. 300–305, 1976.
- [20] P. Sarkar and S. Maitra, "Construction of nonlinear boolean functions with important cryptographic properties," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, pp. 485–506.
- [21] J. Seberry, X.-M. Zhang, and Y. Zheng, "On construction and non-linearity of correlation immune boolean functions," in *Advances in Cryptology—EUROCRYPT 1993 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, pp. 181–199.
- [22] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.
- [23] D. R. Stinson and J. L. Massey, "An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions," *J. Cryptol.*, vol. 8, pp. 167–173, 1995.
- [24] G. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inf. Theory*, pp. 569–571, 1988.
- [25] X.-M. Zhang and Y. Zheng, "On cryptographically resilient functions," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 1740–1747, May 1997.

## The Maximum Squared Correlation, Sum Capacity, and Total Asymptotic Efficiency of Minimum Total-Squared-Correlation Binary Signature Sets

George N. Karystinos, *Member, IEEE*, and  
Dimitris A. Pados, *Member, IEEE*

**Abstract**—The total squared correlation (TSC), maximum squared correlation (MSC), sum capacity ( $C_{\text{sum}}$ ), and total asymptotic efficiency (TAE) of underloaded signature sets, as well as the TSC and  $C_{\text{sum}}$  of overloaded signature sets are metrics that are optimized simultaneously over the real/complex field. In this present work, closed-form expressions are derived for the MSC,  $C_{\text{sum}}$ , and TAE of minimum-TSC binary signature sets. The expressions disprove the general equivalence of these performance metrics over the binary field and establish conditions on the number of signatures and signature length under which simultaneous optimization can or cannot be possible. The sum-capacity loss of the recently designed minimum-TSC binary sets is found to be rather negligible in comparison with minimum-TSC real/complex-valued (Welch-bound-equality) sets.

**Index Terms**—Binary sequences, code-division multiple access (CDMA), code division multiplexing, codes, signal design, spread-spectrum communications, Welch bound.

### I. INTRODUCTION AND BACKGROUND

In direct-sequence code-division-multiple-access (DS-CDMA) systems, individual user signals use distinct signatures (also known as spreading codes) to access a common, in time and frequency, communication channel. In conjunction with channel and receiver design specifics, the overall system performance is determined by the selection of the user signature set. Signature set metrics of interest include the total squared correlation (TSC) [1]–[6], maximum squared correlation (MSC) [1], [2], sum capacity  $C_{\text{sum}}$  [2], and total asymptotic efficiency (TAE) [7], [8]. We recall the definitions of these metrics below.

If

$$\mathbf{S} \triangleq [\mathbf{s}_1 \ \mathbf{s}_2 \ \dots \ \mathbf{s}_K], \quad \mathbf{s}_i \in \mathbb{C}^L, \ \|\mathbf{s}_i\| = 1, \ i = 1, 2, \dots, K$$

is an  $L \times K$  matrix that represents a set of  $K$  normalized (complex-valued in general) user signatures of length (spreading gain)  $L$ , then

- i) the TSC of  $\mathbf{S}$  is the sum of the squared magnitudes of all inner products between signatures

$$\text{TSC}(\mathbf{S}) \triangleq \sum_{i=1}^K \sum_{j=1}^K \left| \mathbf{s}_i^H \mathbf{s}_j \right|^2; \quad (1)$$

Manuscript received February 25, 2003; revised September 14, 2004. This work was supported in part by the National Science Foundation under Grant CCR-0219903 and the U.S. Air Force Office of Scientific Research under Grant FA9550-04-1-0256. The material in this correspondence was presented in part at the Conference on Information Sciences and Systems, Baltimore, MD, March 2003 and in part at IEEE Global Telecommunications Conference, Communications Theory Symposium, San Francisco, CA, December 2003.

G. N. Karystinos was with the Department of Electrical Engineering, State University of New York at Buffalo, Amherst, NY 14260 USA. He is now with the Department of Electrical Engineering, Wright State University, Dayton, OH 45435 USA (e-mail: g.karystinos@wright.edu).

D. A. Pados is with the Department of Electrical Engineering, State University of New York at Buffalo, Amherst, NY 14260 USA (e-mail: pados@eng.buffalo.edu).

Communicated by D. N. C. Tse, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2004.839542

- ii) the MSC of  $\mathbf{S}$  is the maximum squared magnitude among all inner products between distinct signatures

$$\text{MSC}(\mathbf{S}) \triangleq \max_{i \neq j} \left| \mathbf{s}_i^H \mathbf{s}_j \right|^2; \quad (2)$$

- iii) the sum capacity of  $\mathbf{S}$ , defined as the maximum possible sum of user transmission rates with reliable reception, is

$$C_{\text{sum}}(\mathbf{S}) = \log_2 \left| \mathbf{I}_L + \gamma \mathbf{S} \mathbf{S}^H \right| \quad (3)$$

for a common additive white Gaussian noise (AWGN) channel, where  $\gamma$  is the received signal-to-noise-ratio (SNR) of each user signal<sup>1</sup> and  $\mathbf{I}_L$  is the  $L \times L$  identity matrix; and

- iv) the TAE of  $\mathbf{S}$  is equal to the determinant of the signature cross-correlation matrix  $\mathbf{S}^H \mathbf{S}$

$$\text{TAE}(\mathbf{S}) = \left| \mathbf{S}^H \mathbf{S} \right|. \quad (4)$$

In [9], we derived new lower bounds on the TSC of binary antipodal signature sets for all possible combinations of  $K$  (number of users) and  $L$  (signature length) and we proved the tightness of the new bounds for all  $K, L$  except i)  $L = K \equiv 1 \pmod{4}$ , ii)  $L = K \equiv 2 \pmod{4}$ , iii)  $L + 1 = K \equiv 2 \pmod{4}$ , and iv)  $K + 1 = L \equiv 2 \pmod{4}$ . Ding, Golin, and Kløve [10] and Ipatov [11] established the tightness of these bounds also under Cases ii)-iv).<sup>2</sup> All proofs of tightness in [9], as well as in [10], [11], are by construction and present us with simple algorithms for the design of minimum-TSC optimum binary signature sets based on Hadamard matrix transformations. For example, due to these developments, we are now able to design minimum-TSC sets for 99.9% of all possible combinations of  $K, L$  in  $\{1, 2, \dots, 400\}$ .

In this present work, we focus exclusively on binary antipodal signature sets that meet the lower bound on the TSC (minimum-TSC binary sets) [9]. For all  $K$  and  $L$  with  $K \leq L$  (underloaded systems), we derive analytic expressions for the MSC,  $C_{\text{sum}}$ , and TAE of minimum-TSC binary sets. For all  $K$  and  $L$  with  $K \geq L$  (overloaded systems), we derive analytic expressions for the  $C_{\text{sum}}$  of minimum-TSC binary sets. In particular, we show that for all  $K$  and  $L$  (except for  $K = L \equiv 1 \pmod{4}$  that remains an open question), binary minimum-TSC sets possess the following properties: i) if  $K \leq L$ ,  $\text{MSC}(\mathbf{S})$  is also minimum; ii) if  $K \leq L$ ,  $\text{TAE}(\mathbf{S})$  is single-valued when  $L \not\equiv 2 \pmod{4}$  and multi-valued when  $L \equiv 2 \pmod{4}$ ; iii)  $C_{\text{sum}}(\mathbf{S})$  is single-valued when  $\max\{K, L\} \not\equiv 2 \pmod{4}$  and multi-valued when  $\max\{K, L\} \equiv 2 \pmod{4}$ . We derive the exact value of MSC,  $C_{\text{sum}}$ , and TAE when these metrics are single-valued. When  $C_{\text{sum}}$  and/or TAE are multi-valued, we establish lower and upper bounds and prove their tightness; the exact value of  $C_{\text{sum}}$  and/or TAE depends on the particular design of the minimum-TSC signature set. A direct, arguably surprising, conclusion from this study is that minimum-TSC optimal binary sets are not necessarily sum-capacity optimal as known for real-valued sets from the work in [2], [12], [13].

## II. THE MSC OF MINIMUM-TSC BINARY SIGNATURE SETS

We consider a signature matrix  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$  that consists of  $K$  normalized binary antipodal signatures  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i =$

$1, 2, \dots, K$ , where  $L$  is the signature length. The MSC of  $\mathbf{S}$  is defined for every  $K \geq 2$  and is lower-bounded as follows [14]:

$$\text{MSC}(\mathbf{S}) = \max_{i \neq j} \left( \mathbf{s}_i^T \mathbf{s}_j \right)^2 \geq \begin{cases} 0, & L \equiv 0 \pmod{4} \\ \frac{4}{L^2}, & L \equiv 2 \pmod{4} \text{ and } K > 2 \\ 0, & L \equiv 2 \pmod{4} \text{ and } K = 2 \\ \frac{1}{L^2}, & L \equiv 1 \pmod{2}. \end{cases} \quad (5)$$

To examine the MSC of minimum-TSC binary signature sets we state the following lemma. The proof is given in the Appendix.

*Lemma 1:* Let  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$  be an  $L \times K$  binary antipodal signature matrix where  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i = 1, 2, \dots, K$ , and  $K \leq L$ . If  $\text{TSC}(\mathbf{S})$  achieves the lower bound in [9], then there exists an orthogonal matrix  $\mathbf{Q} \in \{-1, 0, 1\}^{K \times K}$  and a matrix  $\mathbf{S}_0 \in \{\pm \frac{1}{\sqrt{L}}\}^{L \times K}$  such that  $\mathbf{S} = \mathbf{S}_0 \mathbf{Q}$  and

$$\mathbf{S}_0^T \mathbf{S}_0 = \begin{cases} \mathbf{I}_K, & L \equiv 0 \pmod{4} \\ \frac{L-1}{L} \mathbf{I}_K + \frac{1}{L} \mathbf{1}_K \mathbf{1}_K^T, & L \equiv 1 \pmod{4} \\ \begin{bmatrix} \mathbf{A}_1 & \mathbf{0}_{K_1 \times K_2} \\ \mathbf{0}_{K_2 \times K_1} & \mathbf{A}_2 \end{bmatrix}, & L \equiv 2 \pmod{4} \\ \frac{L+1}{L} \mathbf{I}_K - \frac{1}{L} \mathbf{1}_K \mathbf{1}_K^T, & L \equiv 3 \pmod{4} \end{cases} \quad (6)$$

where  $\mathbf{1}_K \triangleq [1 \ 1 \ \dots \ 1]^T$ ,  $K_1 \triangleq \lceil \frac{K}{2} \rceil$ ,  $K_2 \triangleq \lfloor \frac{K}{2} \rfloor$ ,  $\mathbf{A}_1$  is a  $K_1 \times K_1$  matrix,  $\mathbf{A}_2$  is a  $K_2 \times K_2$  matrix, and<sup>3</sup>

$$[\mathbf{A}_1]_{ij} = \begin{cases} 1, & i = j \\ \pm \frac{2}{L}, & i \neq j \end{cases}, \quad [\mathbf{A}_2]_{ij} = \begin{cases} 1, & i = j \\ \pm \frac{2}{L}, & i \neq j. \end{cases} \quad \square$$

Consider now a signature matrix  $\mathbf{S}$  with  $1 < K \leq L$  (underloaded system). If  $\text{TSC}(\mathbf{S})$  is equal to the corresponding bound in [9], then by Lemma 1 it is straightforward to obtain

$$\text{MSC}(\mathbf{S}) = \begin{cases} 0, & L \equiv 0 \pmod{4} \\ \frac{4}{L^2}, & L \equiv 2 \pmod{4} \text{ and } K > 2 \\ 0, & L \equiv 2 \pmod{4} \text{ and } K = 2 \\ \frac{1}{L^2}, & L \equiv 1 \pmod{2}. \end{cases} \quad (7)$$

The following proposition summarizes our findings.

*Proposition 1:* If an underloaded binary antipodal signature set achieves the lower bound on the TSC in [9], then it also achieves the lower bound on the MSC in (5).  $\square$

We recall that for underloaded sets ( $K \leq L$ ), the lower bounds on the TSC in [9] are tight for any  $K, L$  subject to the existence of a Hadamard matrix of size  $4 \lfloor \frac{L+2}{4} \rfloor$  with the single exception  $K = L \equiv 1 \pmod{4}$  (see Footnote 2). We conclude that for all  $K, L$  with  $K \leq L$  except  $K = L \equiv 1 \pmod{4}$  that remains an open question in general, i) the minimum-TSC and minimum-MS criteria can be jointly satisfied by the same signature set and ii) the signature sets obtained in [9]–[11] are doubly optimal for underloaded systems: they exhibit both minimum TSC and minimum MSC at the same time. It is important, however, to note at this point that while minimization of the TSC and MSC of real/complex-valued signature sets are *equivalent* criteria for all  $K, L$  with  $K \leq L$ , this is not true in general for binary sets. Specifically, we can show that TSC and MSC minimization are equivalent for binary sets for any  $K, L$  with  $K \leq L$  (subject to the existence of a Hadamard matrix of size  $4 \lfloor \frac{L+2}{4} \rfloor$ ) except for i)

<sup>3</sup>In our notation, if  $\mathbf{A}$  is an  $m \times n$  matrix, then  $[\mathbf{A}]_{ij}$ ,  $i = 1, 2, \dots, m$ ,  $j = 1, 2, \dots, n$ , is the  $(i, j)$ th element of  $\mathbf{A}$ .

<sup>1</sup>In this work, we assume identical received SNR for all user signals.

<sup>2</sup>The case  $K = L \equiv 1 \pmod{4}$  remains open. Ding, Golin, and Kløve [10] showed that our TSC bound in [9] is tight for  $K = L = 5$  or 13, but not for  $K = L = 9$ . What happens when  $K = L = 17, 21, \dots$  is an open question.

$K = L \equiv 1 \pmod{4}$  and ii)  $L \equiv 2 \pmod{4}$ . In particular, when  $L \equiv 2 \pmod{4}$  TSC minimization implies MSC minimization (as shown above) but not *vice versa*.

### III. THE SUM CAPACITY OF MINIMUM-TSC BINARY SIGNATURE SETS

The sum capacity  $C_{\text{sum}}$  of a multiple-access communication channel is the maximum sum of user transmission rates at which reliable decoding at the receiver end is possible [2], [15]. In a synchronous DS-CDMA system that employs an  $L \times K$  complex-valued signature matrix  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$ ,  $\mathbf{s}_i \in \mathbb{C}^L$ ,  $\|\mathbf{s}_i\| = 1$ ,  $i = 1, 2, \dots, K$ , for transmissions over a common AWGN channel, the received data vector is of the form

$$\mathbf{r} = \sum_{i=1}^K d_i \mathbf{s}_i + \mathbf{n} \quad (8)$$

where  $d_i \in \mathbb{C}$ ,  $i = 1, 2, \dots, K$ , is the  $i$ th user's (complex in general) transmitted symbol and  $\mathbf{n}$  is a zero-mean complex Gaussian vector with autocovariance matrix  $N_0 \mathbf{I}_L$ . If  $E\{|d_i|^2\} = E$ ,  $i = 1, 2, \dots, K$ , it is known [2], [7] that

$$C_{\text{sum}}(\mathbf{S}) = \log_2 \left[ \mathbf{I}_L + \gamma \mathbf{S} \mathbf{S}^H \right] \quad (9)$$

where  $\gamma \triangleq \frac{E}{N_0}$  is the received SNR of each user signal. In [2], [12], [13], it was shown that

$$0 \leq C_{\text{sum}}(\mathbf{S}) \leq \begin{cases} K \log_2(1 + \gamma), & K \leq L \\ L \log_2\left(1 + \frac{K}{L} \gamma\right), & K \geq L. \end{cases} \quad (10)$$

While the upper bound in (10) is tight for real/complex-valued signature sets for any  $K, L$  [2], [12], it has been an open question whether tightness is maintained when  $\mathbf{S}$  is binary. In this section, we examine the  $C_{\text{sum}}$  of minimum-TSC binary antipodal signature sets for any  $K, L$ . Our developments are based on the lemma that we state and prove below.

**Lemma 2:** Let  $\mathbf{A}$  be an  $N \times N$  complex Hermitian matrix with the following properties:

- i)  $[\mathbf{A}]_{ii} = \alpha > 0$ ,  $i = 1, 2, \dots, N$ ;
- ii)  $[\mathbf{A}]_{ij} = \beta > 0$ ,  $i \neq j$ ,  $i = 1, 2, \dots, N$ ,  $j = 1, 2, \dots, N$ ;
- iii)  $N < \frac{\alpha}{\beta} + 1$ .

Then, the determinant of  $\mathbf{A}$  is bounded as follows:

$$0 < (\alpha + \beta)^{N-1} (\alpha - (N-1)\beta) \leq |\mathbf{A}| \leq (\alpha - \beta)^{N-1} (\alpha + (N-1)\beta) < \alpha^N. \quad (11)$$

*Proof:* Denote by  $\mathbf{A}_n$  the  $n \times n$  submatrix of  $\mathbf{A}$  that is formed by the first  $n$  columns and the first  $n$  rows of  $\mathbf{A}$ ,  $n = 1, 2, \dots, N$ . Then,

$$\mathbf{A}_{n+1} = \begin{bmatrix} \mathbf{A}_n & \boldsymbol{\rho}_n \\ \boldsymbol{\rho}_n^H & \alpha \end{bmatrix}$$

$\boldsymbol{\rho}_n \in \mathbb{C}^n$ ,  $|\rho_n(i)| = \beta$ ,  $i = 1, 2, \dots, n$ ,  $n = 1, 2, \dots, N-1$ . In particular,  $\mathbf{A}_1 = \alpha$  and  $\mathbf{A}_N = \mathbf{A}$ .

The eigenvalues of  $\mathbf{A}_n$ ,  $\lambda_1, \lambda_2, \dots, \lambda_n$ , are real ( $\mathbf{A}_n$  is Hermitian) and belong to the union of the  $n$  corresponding Gerschgorin circles

<sup>4</sup>Footnote 2 and Proposition 1 show that for  $K = L = 5$  or 13 the MSC bound in (5) is tight and the minimum-TSC binary antipodal signature sets in [10] are doubly optimal. When  $K = L = 9$ , we can prove that the MSC bound in (5) is loose and MSC and TSC cannot be minimized simultaneously by the same binary antipodal signature set.

[16],  $n = 1, 2, \dots, N-1$ . We observe that the  $n$  Gerschgorin circles are identical to each other due to the structure of  $\mathbf{A}_n$ . Therefore,  $|\lambda_i - \alpha| \leq (n-1)\beta$  or  $\lambda_i \in [\alpha - (n-1)\beta, \alpha + (n-1)\beta]$ ,  $i = 1, 2, \dots, n$ . Since  $n \leq N$  and  $N < \frac{\alpha}{\beta} + 1$ , we obtain  $\alpha - (n-1)\beta > 0$ . We conclude that  $\lambda_i > 0$ ,  $i = 1, 2, \dots, n$ ,  $\mathbf{A}_n$  is nonsingular, and the eigenvalues of  $\mathbf{A}_n^{-1}$ ,  $\tilde{\lambda}_1, \tilde{\lambda}_2, \dots, \tilde{\lambda}_n$ , are bounded as follows:

$$0 < \frac{1}{\alpha + (n-1)\beta} \leq \tilde{\lambda}_i \leq \frac{1}{\alpha - (n-1)\beta}, \quad i = 1, 2, \dots, n.$$

Hence,

$$0 < \frac{1}{\alpha + (n-1)\beta} \leq \frac{\boldsymbol{\rho}_n^H \mathbf{A}_n^{-1} \boldsymbol{\rho}_n}{\|\boldsymbol{\rho}_n\|^2} \leq \frac{1}{\alpha - (n-1)\beta}, \quad n = 1, 2, \dots, N-1. \quad (12)$$

We note that  $\|\boldsymbol{\rho}_n\|^2 = n\beta^2$  and recall the identity [16]

$$|\mathbf{A}_{n+1}| = |\mathbf{A}_n| \left( \alpha - \boldsymbol{\rho}_n^H \mathbf{A}_n^{-1} \boldsymbol{\rho}_n \right).$$

From (12), we obtain

$$\alpha - \frac{n\beta^2}{\alpha - (n-1)\beta} \leq \alpha - \boldsymbol{\rho}_n^H \mathbf{A}_n^{-1} \boldsymbol{\rho}_n \leq \alpha - \frac{n\beta^2}{\alpha + (n-1)\beta} < \alpha$$

or

$$\begin{aligned} (\alpha + \beta) \frac{\alpha - n\beta}{\alpha - (n-1)\beta} &\leq \frac{|\mathbf{A}_{n+1}|}{|\mathbf{A}_n|} \\ &\leq (\alpha - \beta) \frac{\alpha + n\beta}{\alpha + (n-1)\beta} < \alpha, \end{aligned} \quad n = 1, 2, \dots, N-1. \quad (13)$$

Since  $1 \leq n \leq N-1$  and  $N < \frac{\alpha}{\beta} + 1$ , we have  $\alpha - n\beta > 0$  and  $\alpha - (n-1)\beta > 0$  for any  $n = 1, 2, \dots, N-1$ . Then

$$\begin{aligned} 0 &< \prod_{n=1}^{N-1} (\alpha + \beta) \frac{\alpha - n\beta}{\alpha - (n-1)\beta} \leq \frac{|\mathbf{A}_N|}{|\mathbf{A}_1|} \\ &\leq \prod_{n=1}^{N-1} (\alpha - \beta) \frac{\alpha + n\beta}{\alpha + (n-1)\beta} < \alpha^{N-1} \end{aligned} \quad (14)$$

which is (11).  $\square$

Consider now a minimum-TSC binary signature matrix  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$  with  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i = 1, 2, \dots, K$ . We use Lemmas 1 and 2 to obtain closed-form expressions for  $C_{\text{sum}}(\mathbf{S})$  for any  $K, L$ . Our developments are presented in the form of the following proposition. The proof is given in the Appendix.

**Proposition 2:** Let  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$ ,  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i = 1, 2, \dots, K$ , be a binary antipodal signature matrix that achieves the TSC lower bound in [9].

a) If  $K \leq L$  (underloaded system)

- i)  $C_{\text{sum}}(\mathbf{S}) = K \log_2(1 + \gamma)$ , if  $L \equiv 0 \pmod{4}$ ;
- ii)  $C_{\text{sum}}(\mathbf{S}) = (K-1) \log_2\left(1 + \frac{L-1}{L} \gamma\right) + \log_2\left(1 + \frac{L+K-1}{L} \gamma\right)$  if  $L \equiv 1 \pmod{4}$ ;
- iii)

$$\begin{aligned} &(K-2) \log_2 \left(1 + \frac{L+2}{L} \gamma\right) + 2 \log_2 \left(1 + \frac{L-K+2}{L} \gamma\right) \\ &\leq C_{\text{sum}}(\mathbf{S}) \end{aligned}$$

$$\leq (K-2) \log_2 \left(1 + \frac{L-2}{L} \gamma\right) + 2 \log_2 \left(1 + \frac{L+K-2}{L} \gamma\right),$$

if  $L \equiv 2 \pmod{4}$ ,  $K \equiv 0 \pmod{2}$ ;

iv)

$$\begin{aligned} &(K-2) \log_2 \left(1 + \frac{L+2}{L} \gamma\right) + \log_2 \left(1 + \frac{L-K+1}{L} \gamma\right) \\ &+ \log_2 \left(1 + \frac{L-K+3}{L} \gamma\right) \end{aligned}$$

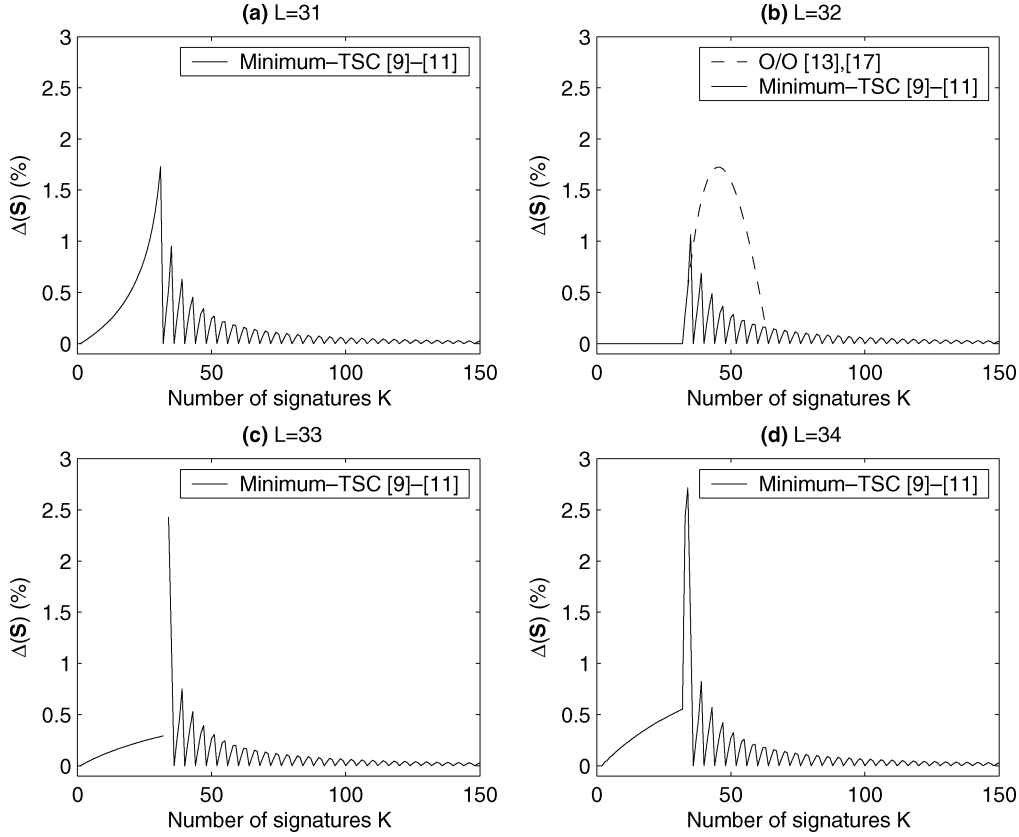


Fig. 1. Sum-capacity loss  $\Delta(\mathbf{S})$  (%) of minimum-TSC and O/O binary signature sets versus number of signatures  $K$  of length (a)  $L = 31$ , (b)  $L = 32$ , (c)  $L = 33$ , and (d)  $L = 34$  ( $\gamma = 12$  dB).

$$\begin{aligned} &\leq C_{\text{sum}}(\mathbf{S}) \\ &\leq (K-2)\log_2\left(1 + \frac{L-2}{L}\gamma\right) + \log_2\left(1 + \frac{L+K-1}{L}\gamma\right) \\ &\quad + \log_2\left(1 + \frac{L+K-3}{L}\gamma\right), \end{aligned}$$

if  $L \equiv 2 \pmod{4}$ ,  $K \equiv 1 \pmod{2}$ ;

$$\text{v) } C_{\text{sum}}(\mathbf{S}) = (K-1)\log_2\left(1 + \frac{L+1}{L}\gamma\right) + \log_2\left(1 + \frac{L-K+1}{L}\gamma\right),$$

if  $L \equiv 3 \pmod{4}$ .

When  $L \equiv 2 \pmod{4}$ , the lower bounds in iii), iv) are tight if there exists a Hadamard matrix of size  $L+2$  while the upper bounds are tight if  $K \leq L-2$  and there exists a Hadamard matrix of size  $L-2$ .

b) If  $K \geq L$  (overloaded system)

$$\begin{aligned} \text{i) } &C_{\text{sum}}(\mathbf{S}) = L\log_2\left(1 + \frac{K}{L}\gamma\right), \text{ if } K \equiv 0 \pmod{4}; \\ \text{ii) } &C_{\text{sum}}(\mathbf{S}) = (L-1)\log_2\left(1 + \frac{K-1}{L}\gamma\right) + \log_2\left(1 + \frac{K+L-1}{L}\gamma\right), \\ &\text{if } K \equiv 1 \pmod{4}; \end{aligned}$$

iii)

$$\begin{aligned} &(L-2)\log_2\left(1 + \frac{K+2}{L}\gamma\right) + 2\log_2\left(1 + \frac{K-L+2}{L}\gamma\right) \\ &\leq C_{\text{sum}}(\mathbf{S}) \\ &\leq (L-2)\log_2\left(1 + \frac{K-2}{L}\gamma\right) + 2\log_2\left(1 + \frac{K+L-2}{L}\gamma\right), \end{aligned}$$

if  $K \equiv 2 \pmod{4}$ ,  $L \equiv 0 \pmod{2}$ ;

iv)

$$\begin{aligned} &(L-2)\log_2\left(1 + \frac{K+2}{L}\gamma\right) + \log_2\left(1 + \frac{K-L+1}{L}\gamma\right) \\ &\quad + \log_2\left(1 + \frac{K-L+3}{L}\gamma\right) \\ &\leq C_{\text{sum}}(\mathbf{S}) \end{aligned}$$

$$\begin{aligned} &\leq (L-2)\log_2\left(1 + \frac{K-2}{L}\gamma\right) + \log_2\left(1 + \frac{K+L-1}{L}\gamma\right) \\ &\quad + \log_2\left(1 + \frac{K+L-3}{L}\gamma\right), \end{aligned}$$

if  $K \equiv 2 \pmod{4}$ ,  $L \equiv 1 \pmod{2}$ ;

$$\text{v) } C_{\text{sum}}(\mathbf{S}) = (L-1)\log_2\left(1 + \frac{K+1}{L}\gamma\right) + \log_2\left(1 + \frac{K-L+1}{L}\gamma\right),$$

if  $K \equiv 3 \pmod{4}$ .

When  $K \equiv 2 \pmod{4}$ , the lower bounds in iii), iv) are tight if there exists a Hadamard matrix of size  $K+2$  while the upper bounds are tight if  $K \geq L+2$  and there exists a Hadamard matrix of size  $K-2$ .  $\square$

To visualize the theoretical developments of Proposition 2 on the sum capacity of binary signature sets, we consider the relative sum-capacity loss expression

$$\Delta(\mathbf{S}) \triangleq 1 - \frac{C_{\text{sum}}(\mathbf{S})}{C_{\text{sum}}^*}$$

where  $C_{\text{sum}}^*$  is the sum capacity of a real/complex-valued Welch-bound-equality (WBE) signature set of the same size as  $\mathbf{S}$ . In Fig. 1, we plot the sum-capacity loss  $\Delta(\mathbf{S})$  of minimum-TSC binary sets as a function of  $K$  for a common received SNR per user  $\gamma = 12$  dB and four different signature length values  $L = 31, 32, 33$ , and  $34$ . For  $L = 32$  (Fig. 1(b)) and  $L \leq K \leq 2L$ , we also include the sum-capacity loss of the binary ‘‘O/O signature sets’’ designed in [17].<sup>5</sup> We observe that binary minimum-TSC sets exhibit rather negligible sum-capacity loss for almost all  $K, L$  of Fig. 1 (with  $\gamma = 12$  dB) in comparison with WBE real/complex-valued sets. In addition,

<sup>5</sup>In [17] Vanhaverbeke, Moeneclaey, and Sari designed binary signature sets for lengths  $L \equiv 0 \pmod{4}$  and number of signatures  $K = L, L+1, \dots, 2L$  which they named OCDMA/OCDMA (O/O) sequence sets. The sum capacity of the O/O sets was studied in [13].

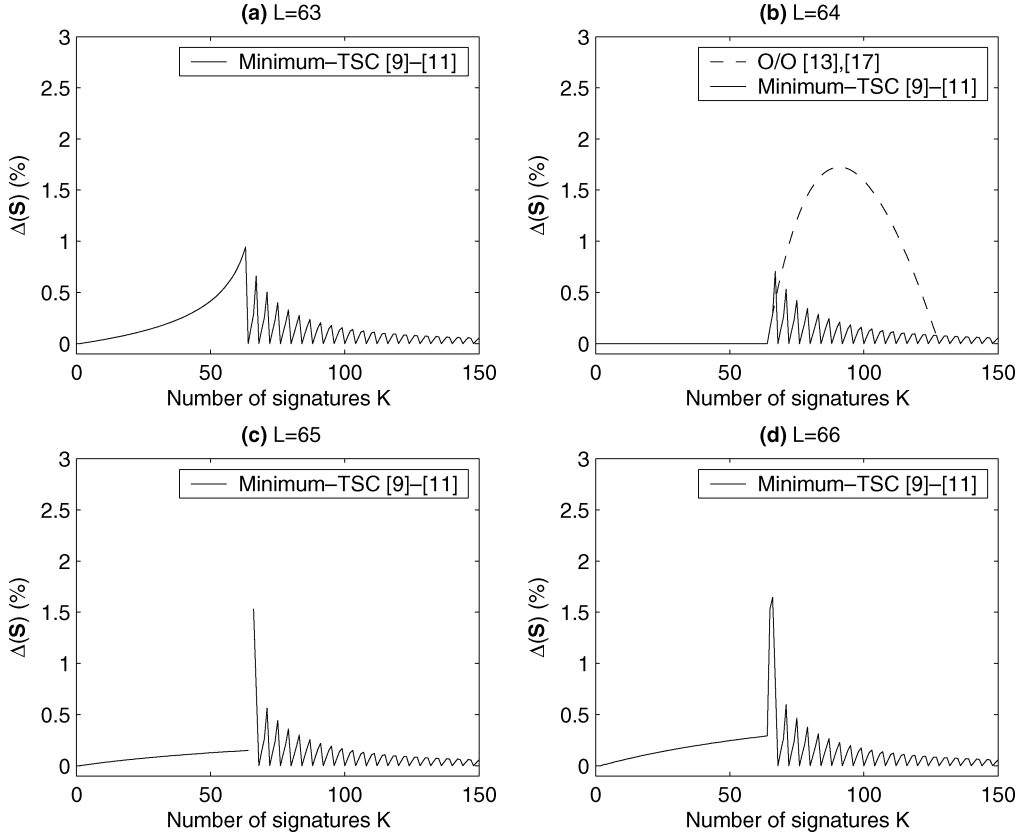


Fig. 2. Sum-capacity loss  $\Delta(\mathbf{S})$  (%) of minimum-TSC and O/O binary signature sets versus number of signatures  $K$  of length (a)  $L = 63$ , (b)  $L = 64$ , (c)  $L = 65$ , and (d)  $L = 66$  ( $\gamma = 12$  dB).

when  $L = 32$ , the sum-capacity loss of binary minimum-TSC sets is significantly less than the sum-capacity loss of O/O sets [13], [17] for almost all values of  $K = 32, 33, \dots, 64$ . Yet, the existence of a single pair  $(K, L) = (35, 32)$  in Fig. 1(b) for which the corresponding nonminimum-TSC O/O set in [13], [17] exhibits higher sum-capacity than *any* binary minimum-TSC set of the same size proves that minimum-TSC and maximum- $C_{\text{sum}}$  criteria are not equivalent for binary sets. We recall that binary minimum-TSC sets with the sum-capacity performance presented in Fig. 1 can be designed from [9]–[11] for any  $K, L$  except  $K = L \equiv 1 \pmod{4}$ . This explains the missing sum-capacity performance point  $K = L = 33$  in Fig. 1(c).

In Fig. 2, we repeat the same study of Fig. 1 for  $L = 63, 64, 65$ , and  $66$ . Similar conclusions may be drawn. Notice the  $(K = 67, L = 64)$  point in Fig. 2(b) for which the  $C_{\text{sum}}$  of the O/O sets is higher than that of all minimum-TSC sets. Notice also the missing  $K = L = 65$  minimum-TSC point in Fig. 2(c).

#### IV. THE TOTAL ASYMPTOTIC EFFICIENCY OF MINIMUM-TSC BINARY SIGNATURE SETS

The  $\text{TAE}(\mathbf{S}) = |\mathbf{S}^H \mathbf{S}|$  of a complex-valued signature matrix  $\mathbf{S} = [\mathbf{s}_1 \ \mathbf{s}_2 \ \dots \ \mathbf{s}_K]$ ,  $\mathbf{s}_i \in \mathbb{C}^L$ ,  $\|\mathbf{s}_i\| = 1$ ,  $i = 1, 2, \dots, K$ , is real-valued [16] and bounded as follows:

$$0 \leq \text{TAE}(\mathbf{S}) \leq 1. \quad (15)$$

The unit upper bound in (15) is readily proved via Hadamard's inequality [15]. We also note that if  $K > L$  (overloaded system),  $\mathbf{S}^H \mathbf{S}$  is rank-deficient and  $\text{TAE}(\mathbf{S}) = 0$ .

While the upper bound in (15) is tight for real/complex-valued signature sets for any  $K, L$  with  $K \leq L$  [7], [8], it has been an open

question whether tightness is maintained when  $\mathbf{S}$  is binary antipodal, that is,  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i = 1, 2, \dots, K$ . To connect with the  $C_{\text{sum}}$  developments of the previous section, it is straightforward to show that

$$\text{TAE}(\mathbf{S}) = \lim_{\gamma \rightarrow \infty} \frac{2^{C_{\text{sum}}(\mathbf{S})}}{\gamma^K} \quad (16)$$

for any  $K, L$  with  $K \leq L$ . Of course, (16) does not necessarily imply that TAE increases monotonically with  $C_{\text{sum}}$  for fixed  $\gamma$ . In fact, one can find two binary signature sets  $\mathbf{S}_1$  and  $\mathbf{S}_2$  with  $\text{TAE}(\mathbf{S}_1) > \text{TAE}(\mathbf{S}_2)$  while  $C_{\text{sum}}(\mathbf{S}_1) > C_{\text{sum}}(\mathbf{S}_2)$  or  $C_{\text{sum}}(\mathbf{S}_1) < C_{\text{sum}}(\mathbf{S}_2)$  depending on the exact value of  $\gamma$ . In this section, we obtain closed-form expressions for the TAE of minimum-TSC binary antipodal signature sets with  $K \leq L$  (underloaded system). Our developments are presented in the form of the following proposition. The proof is obtained directly from Proposition 2 and (16) and is, therefore, omitted.

*Proposition 3:* Let  $\mathbf{S} = [\mathbf{s}_1 \ \mathbf{s}_2 \ \dots \ \mathbf{s}_K]$  be a binary antipodal signature matrix where  $\mathbf{s}_i \in \{\pm \frac{1}{\sqrt{L}}\}^L$ ,  $i = 1, 2, \dots, K$ , and  $K \leq L$ . If  $\text{TSC}(\mathbf{S})$  achieves the lower bound in [9], then

- i)  $\text{TAE}(\mathbf{S}) = 1$ , if  $L \equiv 0 \pmod{4}$ ;
- ii)  $\text{TAE}(\mathbf{S}) = \frac{(L-1)^{K-1}(L+K-1)}{L^K}$ , if  $L \equiv 1 \pmod{4}$ ;
- iii)

$$\begin{aligned} & \frac{(L+2)^{K-2}(L-K+2)^2}{L^K} \\ & \leq \text{TAE}(\mathbf{S}) \\ & \leq \frac{(L-2)^{K-2}(L+K-2)^2}{L^K} \end{aligned}$$

if  $L \equiv 2 \pmod{4}$ ,  $K \equiv 0 \pmod{2}$ ;

iv)

$$\begin{aligned} & \frac{(L+2)^{K-2}(L-K+1)(L-K+3)}{L^K} \\ & \leq \text{TAE}(\mathbf{S}) \\ & \leq \frac{(L-2)^{K-2}(L+K-1)(L+K-3)}{L^K} \end{aligned}$$

 if  $L \equiv 2 \pmod{4}$ ,  $K \equiv 1 \pmod{2}$ ;

 v)  $\text{TAE}(\mathbf{S}) = \frac{(L+1)^{K-1}(L-K+1)}{L^K}$ , if  $L \equiv 3 \pmod{4}$ .

When  $L \equiv 2 \pmod{4}$ , the lower bounds in iii), iv) are tight if there exists a Hadamard matrix of size  $L+2$  while the upper bounds are tight if  $K \leq L-2$  and there exists a Hadamard matrix of size  $L-2$ .  $\square$

We recall that for real/complex-valued sets TAE maximization and TSC minimization are equivalent problems for all  $K, L$  with  $K \leq L$  [8]. As shown by Proposition 3, however, this property no longer holds true for binary antipodal sets. If  $L \equiv 2 \pmod{4}$  and  $K \leq L-2$ , then there exist minimum-TSC sets that do not have maximum TAE. Whether the TAE values of minimum-TSC binary sets in ii), v) and the upper bounds in iii), iv) of Proposition 3 are also upper bounds on the TAE of any binary antipodal signature set is an interesting open question.

## V. CONCLUSION

In an effort to gain better understanding of the theoretical intricacies of code-division multiplexing, we looked at the following four signature performance metrics: Total squared correlation (TSC), maximum squared correlation (MSC), sum capacity ( $C_{\text{sum}}$ ), and total asymptotic efficiency (TAE). For real/complex-valued signature sets, all four optimization criteria are equivalent. Real/complex-valued minimum-TSC sets are minimum-MSC and maximum-TAE when the number of signatures  $K$  is less than or equal to the signature length  $L$  and have maximum sum-capacity for any  $K, L$ .

In this correspondence, based on our recent developments on the TSC of binary antipodal signature sets, we derived closed-form expressions for the MSC,  $C_{\text{sum}}$ , and TAE value that binary minimum-TSC sets achieve for all  $K, L$  with  $K \leq L$  except  $K = L \equiv 1 \pmod{4}$  and the  $C_{\text{sum}}$  value that binary minimum-TSC sets achieve for all  $K, L$  with  $K > L$ . Interestingly, there exist  $K, L$  values for which different metrics are optimized by different binary sets.

It remains to be examined whether—and if so under which conditions—the expressions that we derived in this correspondence represent upper bounds on the  $C_{\text{sum}}$  and TAE of any binary antipodal signature set. For the moment, we can say that the minimum-TSC binary sets designed in [9]–[11] exhibit rather negligible sum-capacity loss in comparison with real/complex-valued optimum WBE sets.

## APPENDIX I PROOF OF LEMMA 1

We define the Hamming distance

$$d(\mathbf{s}_i, \mathbf{s}_j) \triangleq |\{l : \mathbf{s}_i(l) \neq \mathbf{s}_j(l), l = 1, 2, \dots, L\}|$$

between  $\mathbf{s}_i, \mathbf{s}_j \in \{\pm \frac{1}{\sqrt{L}}\}^L$  where  $|\cdot|$  denotes set cardinality. The cross-correlation and the Hamming distance between any two vectors  $\mathbf{s}_i, \mathbf{s}_j$  in  $\mathbf{S} = [\mathbf{s}_1 \mathbf{s}_2 \dots \mathbf{s}_K]$  are related as follows:

$$d(\mathbf{s}_i, \mathbf{s}_j) = \frac{L}{2} (1 - \mathbf{s}_i^T \mathbf{s}_j). \quad (17)$$

Consider any three vectors  $\mathbf{s}_i, \mathbf{s}_j$ , and  $\mathbf{s}_k$  in  $\mathbf{S}$ . Then

$$\begin{aligned} d(\mathbf{s}_j, \mathbf{s}_k) &= d(\mathbf{s}_j, \mathbf{s}_i) + d(\mathbf{s}_i, \mathbf{s}_k) \\ &- 2|\{l : \mathbf{s}_j(l) \neq \mathbf{s}_i(l) \text{ and } \mathbf{s}_i(l) \neq \mathbf{s}_k(l), l = 1, 2, \dots, L\}|. \end{aligned} \quad (18)$$

Using (17) we obtain

$$L\mathbf{s}_j^T \mathbf{s}_k \equiv L\mathbf{s}_j^T \mathbf{s}_i + L\mathbf{s}_i^T \mathbf{s}_k - L \pmod{4}. \quad (19)$$

*Case  $L \equiv 0 \pmod{4}$ :* It can be shown [9] that  $\mathbf{s}_i^T \mathbf{s}_j = 0 \forall i \neq j$ . Therefore,  $\mathbf{S}^T \mathbf{S} = \mathbf{I}_K$ . Set  $\mathbf{S}_0 = \mathbf{S}$  and  $\mathbf{Q} = \mathbf{I}_K$ . Then,  $\mathbf{S} = \mathbf{S}_0 \mathbf{Q}$  and  $\mathbf{S}_0^T \mathbf{S}_0 = \mathbf{I}_K$ .

*Case  $L \equiv 1 \pmod{4}$ :* In [9], it was shown that  $|\mathbf{s}_i^T \mathbf{s}_j| = \frac{1}{L} \forall i \neq j$ . Hence,  $L\mathbf{s}_i^T \mathbf{s}_j = \pm 1$ .

Choose an arbitrary signature in  $\mathbf{S}$ , say  $\mathbf{s}_1$ , and partition  $\mathbf{S}$  into two signature matrices  $\mathbf{S}_1$  and  $\mathbf{S}_2$  of size  $L \times K_1$  and  $L \times K_2$ , respectively, as follows:

$$\mathbf{s}_1 \in \mathbf{S}_1 \text{ and } \mathbf{s}_i \in \begin{cases} \mathbf{S}_1, & \text{if } L\mathbf{s}_1^T \mathbf{s}_i = 1 \\ \mathbf{S}_2, & \text{if } L\mathbf{s}_1^T \mathbf{s}_i = -1 \end{cases}, i = 2, 3, \dots, K. \quad (20)$$

Consider any two signatures  $\mathbf{s}_i, \mathbf{s}_j, i \neq j$ , in  $\mathbf{S}_1$  other than  $\mathbf{s}_1$ . Let  $L = 4m + 1, m \in \{0, 1, 2, \dots\}$ . Then, by (19)

$$L\mathbf{s}_i^T \mathbf{s}_j \equiv 1 + 1 - (4m + 1) \equiv 1 \pmod{4}.$$

We know, in addition, that  $L\mathbf{s}_i^T \mathbf{s}_j = \pm 1$ . We conclude that

$$L[\mathbf{S}_1^T \mathbf{S}_1]_{ij} = 1, \quad i \neq j = 1, \dots, K_1$$

or

$$L\mathbf{S}_1^T \mathbf{S}_1 = (L-1)\mathbf{I}_{K_1} + \mathbf{1}_{K_1 \times K_1} \quad (21)$$

where  $\mathbf{1}_{K_1 \times K_2} \triangleq \mathbf{1}_{K_1} \mathbf{1}_{K_2}^T$ . Similarly, we can show that

$$L\mathbf{S}_2^T \mathbf{S}_2 = (L-1)\mathbf{I}_{K_2} + \mathbf{1}_{K_2 \times K_2} \quad (22)$$

and

$$L\mathbf{S}_1^T \mathbf{S}_2 = -\mathbf{1}_{K_1 \times K_2}. \quad (23)$$

Consider a  $K \times K$  permutation (orthogonal) matrix  $\mathbf{Q}_1$  such that  $\mathbf{S}\mathbf{Q}_1 = [\mathbf{S}_1 \mathbf{S}_2]$  and the orthogonal matrix

$$\mathbf{Q}_2 \triangleq \begin{bmatrix} \mathbf{I}_{K_1} & \mathbf{0}_{K_1 \times K_2} \\ \mathbf{0}_{K_2 \times K_1} & -\mathbf{I}_{K_2} \end{bmatrix}.$$

Set  $\mathbf{Q} \triangleq (\mathbf{Q}_1 \mathbf{Q}_2)^T$  and  $\mathbf{S}_0 \triangleq \mathbf{S}\mathbf{Q}^T$ .  $\mathbf{Q}$  is orthogonal and  $\mathbf{S} = \mathbf{S}_0 \mathbf{Q}$ . Also,  $\mathbf{S}_0 = \mathbf{S}\mathbf{Q}_1 \mathbf{Q}_2 = [\mathbf{S}_1 - \mathbf{S}_2]$ . Therefore,

$$\begin{aligned} L\mathbf{S}_0^T \mathbf{S}_0 &= L \begin{bmatrix} \mathbf{S}_1^T \\ -\mathbf{S}_2^T \end{bmatrix} [\mathbf{S}_1 - \mathbf{S}_2] \\ &= \begin{bmatrix} (L-1)\mathbf{I}_{K_1} + \mathbf{1}_{K_1 \times K_1} & \mathbf{1}_{K_1 \times K_2} \\ \mathbf{1}_{K_2 \times K_1} & (L-1)\mathbf{I}_{K_2} + \mathbf{1}_{K_2 \times K_2} \end{bmatrix} \\ &= (L-1)\mathbf{I}_K + \mathbf{1}_{K \times K}. \end{aligned} \quad (24)$$

*Case  $L \equiv 2 \pmod{4}$ :* In [9], it was shown that  $\mathbf{S}$  can be partitioned into two signature matrices  $\mathbf{S}_1$  and  $\mathbf{S}_2$  of size  $L \times \lceil \frac{K}{2} \rceil$  and  $L \times \lfloor \frac{K}{2} \rfloor$ , respectively, such that

$$[\mathbf{S}_1^T \mathbf{S}_1]_{ij} = \begin{cases} 1, & i = j \\ \pm \frac{2}{L}, & i \neq j \end{cases}, \quad [\mathbf{S}_2^T \mathbf{S}_2]_{ij} = \begin{cases} 1, & i = j \\ \pm \frac{2}{L}, & i \neq j \end{cases}$$

and

$$\mathbf{S}_1^T \mathbf{S}_2 = \mathbf{0}_{\lceil \frac{K}{2} \rceil \times \lfloor \frac{K}{2} \rfloor}. \quad (25)$$

Set  $\mathbf{A}_1 \triangleq \mathbf{S}_1^T \mathbf{S}_1$ ,  $\mathbf{A}_2 \triangleq \mathbf{S}_2^T \mathbf{S}_2$ ,  $\mathbf{S}_0 \triangleq [\mathbf{S}_1 \ \mathbf{S}_2]$ , and consider a  $K \times K$  permutation (orthogonal) matrix  $\mathbf{Q}$  such that  $\mathbf{S}\mathbf{Q}^T = [\mathbf{S}_1 \ \mathbf{S}_2]$ . Then,  $\mathbf{S} = \mathbf{S}_0\mathbf{Q}$  and

$$\begin{aligned} \mathbf{S}_0^T \mathbf{S}_0 &= \begin{bmatrix} \mathbf{S}_1^T \mathbf{S}_1 & \mathbf{0}_{\lceil \frac{K}{2} \rceil \times \lceil \frac{K}{2} \rceil} \\ \mathbf{0}_{\lceil \frac{K}{2} \rceil \times \lceil \frac{K}{2} \rceil} & \mathbf{S}_2^T \mathbf{S}_2 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{A}_1 & \mathbf{0}_{\lceil \frac{K}{2} \rceil \times \lceil \frac{K}{2} \rceil} \\ \mathbf{0}_{\lceil \frac{K}{2} \rceil \times \lceil \frac{K}{2} \rceil} & \mathbf{A}_2 \end{bmatrix}. \end{aligned} \quad (26)$$

Case  $L \equiv 3 \pmod{4}$ : The proof is similar to the proof for the Case  $L \equiv 1 \pmod{4}$  and omitted for brevity in presentation.  $\square$

## APPENDIX II PROOF OF PROPOSITION 2

### A. Part a)

By Lemma 1, we can write  $\mathbf{S} = \mathbf{S}_0\mathbf{Q}$  where  $\mathbf{Q} \in \{-1, 0, 1\}^{K \times K}$  and is orthogonal and  $\mathbf{S}_0 \in \{\pm \frac{1}{\sqrt{L}}\}^{L \times K}$ . Then

$$\begin{aligned} C_{\text{sum}}(\mathbf{S}) &= \log_2 |\mathbf{I}_L + \gamma \mathbf{S}\mathbf{S}^T| = \log_2 |\mathbf{I}_K + \gamma \mathbf{S}^T \mathbf{S}| \\ &= \log_2 |\mathbf{Q}^T \mathbf{Q} + \gamma \mathbf{Q}^T \mathbf{S}_0^T \mathbf{S}_0 \mathbf{Q}| \\ &= \log_2 |\mathbf{I}_K + \gamma \mathbf{S}_0^T \mathbf{S}_0|. \end{aligned}$$

Therefore, it suffices to examine  $\log_2 |\mathbf{I}_K + \gamma \mathbf{S}_0^T \mathbf{S}_0|$ .

i) By Lemma 1,  $\mathbf{S}_0^T \mathbf{S}_0 = \mathbf{I}_K$ . Therefore,

$$\log_2 |\mathbf{I}_K + \gamma \mathbf{S}_0^T \mathbf{S}_0| = \log_2 |(1 + \gamma) \mathbf{I}_K| = K \log_2 (1 + \gamma). \quad (27)$$

ii) By Lemma 1,  $\mathbf{S}_0^T \mathbf{S}_0 = \frac{L-1}{L} \mathbf{I}_K + \frac{1}{L} \mathbf{1}_K \mathbf{1}_K^T$ . Therefore,

$$\begin{aligned} \log_2 |\mathbf{I}_K + \gamma \mathbf{S}_0^T \mathbf{S}_0| &= \log_2 \left| \left(1 + \frac{L-1}{L} \gamma\right) \mathbf{I}_K + \frac{\gamma}{L} \mathbf{1}_K \mathbf{1}_K^T \right| \\ &= \log_2 \left( \left(1 + \frac{L-1}{L} \gamma\right)^K \left| \mathbf{I}_K + \frac{\frac{\gamma}{L}}{1 + \frac{L-1}{L} \gamma} \mathbf{1}_K \mathbf{1}_K^T \right| \right) \\ &= \log_2 \left( \left(1 + \frac{L-1}{L} \gamma\right)^K \left(1 + \frac{\frac{\gamma}{L}}{1 + \frac{L-1}{L} \gamma} \|\mathbf{1}_K\|^2\right) \right) \\ &= (K-1) \log_2 \left(1 + \frac{L-1}{L} \gamma\right) + \log_2 \left(1 + \frac{L+K-1}{L} \gamma\right). \end{aligned} \quad (28)$$

iii) By Lemma 1

$$\begin{aligned} \log_2 |\mathbf{I}_K + \gamma \mathbf{S}_0^T \mathbf{S}_0| &= \log_2 \left| \begin{bmatrix} \mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_1 & \mathbf{0}_{\frac{K}{2} \times \frac{K}{2}} \\ \mathbf{0}_{\frac{K}{2} \times \frac{K}{2}} & \mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_2 \end{bmatrix} \right| \\ &= \log_2 |\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_1| \log_2 |\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_2| \end{aligned} \quad (29)$$

where  $\mathbf{A}_1, \mathbf{A}_2$  are  $\frac{K}{2} \times \frac{K}{2}$  matrices and

$$\begin{aligned} \left[\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_1\right]_{ij} &= \begin{cases} 1 + \gamma, & i = j \\ \pm \frac{2\gamma}{L}, & i \neq j \end{cases} \\ \left[\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_2\right]_{ij} &= \begin{cases} 1 + \gamma, & i = j \\ \pm \frac{2\gamma}{L}, & i \neq j. \end{cases} \end{aligned}$$

Set  $\alpha = 1 + \gamma, \beta = \frac{2\gamma}{L}$ , observe that  $\frac{K}{2} < \frac{\alpha}{\beta} + 1$ , and use Lemma 2 to obtain

$$\begin{aligned} &\left(\frac{K}{2} - 1\right) \log_2 \left(1 + \gamma + \frac{2\gamma}{L}\right) \\ &\quad + \log_2 \left(1 + \gamma - \left(\frac{K}{2} - 1\right) \frac{2\gamma}{L}\right) \\ &\leq \log_2 |\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_1| \\ &\leq \left(\frac{K}{2} - 1\right) \log_2 \left(1 + \gamma - \frac{2\gamma}{L}\right) \\ &\quad + \log_2 \left(1 + \gamma + \left(\frac{K}{2} - 1\right) \frac{2\gamma}{L}\right) \\ &< \frac{K}{2} \log_2 (1 + \gamma) \end{aligned} \quad (30)$$

$$\begin{aligned} &\left(\frac{K}{2} - 1\right) \log_2 \left(1 + \gamma + \frac{2\gamma}{L}\right) \\ &\quad + \log_2 \left(1 + \gamma - \left(\frac{K}{2} - 1\right) \frac{2\gamma}{L}\right) \\ &\leq \log_2 |\mathbf{I}_{\frac{K}{2}} + \gamma \mathbf{A}_2| \\ &\leq \left(\frac{K}{2} - 1\right) \log_2 \left(1 + \gamma - \frac{2\gamma}{L}\right) \\ &\quad + \log_2 \left(1 + \gamma + \left(\frac{K}{2} - 1\right) \frac{2\gamma}{L}\right) \\ &< \frac{K}{2} \log_2 (1 + \gamma). \end{aligned} \quad (31)$$

Direct addition of the inequalities (30) and (31) results to the bounds on  $C_{\text{sum}}(\mathbf{S})$  as they appear in Proposition 2, Part a), Case iii). The tightness of these bounds depends on the existence of Hadamard matrices of size  $L-2$  and  $L+2$ . If a size  $L-2$  Hadamard matrix exists and  $K \leq L-2$ , then the signature design method in [9] provides us with minimum-TSC sets whose  $C_{\text{sum}}$  achieves the upper bound of Case iii) of Proposition 2, Part a). If a size  $L+2$  Hadamard matrix exists, then the minimum-TSC sets designed in [10], [11] have  $C_{\text{sum}}$  equal to the lower bound of Case iii) of Proposition 2, Part a).

iv) The proof is similar to the proof for the Case iii) and omitted for brevity in presentation.

v) The proof is similar to the proof for the Case ii) and omitted for brevity in presentation.

### B. Part b)

Set  $\mathbf{D} \triangleq \sqrt{\frac{L}{K}} \mathbf{S}^T$ . Then

$$\begin{aligned} C_{\text{sum}}(\mathbf{S}) &= \log_2 |\mathbf{I}_L + \gamma \mathbf{S}\mathbf{S}^T| = \log_2 \left| \mathbf{I}_L + \frac{\gamma K}{L} \mathbf{D}^T \mathbf{D} \right| \\ &= \log_2 \left| \mathbf{I}_K + \frac{\gamma K}{L} \mathbf{D} \mathbf{D}^T \right|. \end{aligned}$$

$\mathbf{D} \in \{\pm \frac{1}{\sqrt{K}}\}^{K \times L}$  can be viewed as a signature matrix with  $L$  unit-norm binary signatures of length  $K \geq L$ . Therefore,  $C_{\text{sum}}(\mathbf{S})$  at SNR  $\gamma$  equals  $C_{\text{sum}}(\mathbf{D})$  at SNR  $\frac{\gamma K}{L}$  where  $\mathbf{S}$  is overloaded and  $\mathbf{D}$  is the corresponding underloaded set. We can show that if TSC( $\mathbf{S}$ ) achieves the TSC lower bound for overloaded sets in [9], then TSC( $\mathbf{D}$ ) achieves the TSC lower bound for underloaded sets in [9]. Hence, we can apply our results in Part a) of Proposition 2 to  $\mathbf{D}$  and obtain the  $C_{\text{sum}}(\mathbf{S})$  expressions in all five cases of Proposition 2, Part b), directly. We note that

the tightness of the bounds on  $C_{\text{sum}}(\mathbf{S})$  when  $L \leq K \equiv 2 \pmod{4}$  (Cases iii) and iv)) depends on the existence of Hadamard matrices of size  $K - 2$  and  $K + 2$ . Indeed, if a size  $K - 2$  Hadamard matrix exists and  $K \geq L + 2$ , then the signature design method in [9] provides us with minimum-TSC sets whose  $C_{\text{sum}}$  achieves the upper bound in Case iii) or iv) of Proposition 2, Part b). If a size  $K + 2$  Hadamard matrix exists, then the minimum-TSC sets designed in [10], [11] have  $C_{\text{sum}}$  equal to the lower bound in Case iii) or iv) of Proposition 2, Part b).  $\square$

## REFERENCES

- [1] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.
- [2] M. Rupp and J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1261–1266, Jul. 1994.
- [3] P. Viswanath, V. Anantharam, and D. N. C. Tse, "Optimal sequences, power control, and user capacity of synchronous CDMA systems with linear MMSE multiuser receivers," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1968–1983, Sep. 1999.
- [4] P. Cota, "An algorithm for obtaining Welch bound equality sequences for S-CDMA channels," *AEU. Int. J. Electron. Commun.*, vol. 55, pp. 95–99, Mar. 2001.
- [5] S. Ulukus and R. D. Yates, "Iterative construction of optimum signature sequence sets in synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1989–1998, Jul. 2001.
- [6] C. Rose, "CDMA codeword optimization: Interference avoidance and convergence via class warfare," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2368–2382, Sep. 2001.
- [7] S. Verdú, "Capacity region of Gaussian CDMA channels: The symbol-synchronous case," in *Proc. 24th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, Oct. 1986, pp. 1025–1034.
- [8] D. Parsavand and M. K. Varanasi, "RMS bandwidth constrained signature waveforms that maximize the total capacity of PAM-synchronous CDMA channels," *IEEE Trans. Commun.*, vol. 44, no. 1, pp. 65–75, Jan. 1996.
- [9] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-SS binary signature sets," *IEEE Trans. Commun.*, vol. 51, no. 1, pp. 48–51, Jan. 2003.
- [10] C. Ding, M. Golin, and T. Klöve, "Meeting the Welch and Karystinos-Pados bounds on DS-SS binary signature sets," *Des., Codes Cryptogr.*, vol. 30, pp. 73–84, Aug. 2003.
- [11] V. P. Ipatov, "On the Karystinos-Pados bounds and optimal binary DS-SS signature ensembles," *IEEE Commun. Lett.*, vol. 8, no. 2, pp. 81–83, Feb. 2004.
- [12] P. Viswanath and V. Anantharam, "Optimal sequences and sum capacity of synchronous CDMA systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1984–1991, Sep. 1999.
- [13] F. Vanhaverbeke and M. Moeneclaey, "Sum capacity of the OCDMA/OCDMA signature sequence set," *IEEE Commun. Lett.*, vol. 6, no. 8, pp. 340–342, Aug. 2002.
- [14] G. N. Karystinos and D. A. Pados, "Binary CDMA signature sets with concurrently minimum total-squared-correlation and maximum-squared-correlation," in *Proc. 2003 IEEE Int. Conf. Communications*, vol. 4, Anchorage, AK, May 2003, pp. 2500–2503.
- [15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [16] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Philadelphia, PA: SIAM, 2000.
- [17] F. Vanhaverbeke, M. Moeneclaey, and H. Sari, "DS/SS with two sets of orthogonal spreading sequences and iterative detection," *IEEE Commun. Lett.*, vol. 4, no. 9, pp. 289–291, Sep. 2000.

## A Counterexample for the Open Problem on the Minimal Delays of Orthogonal Designs With Maximal Rates

Haibin Kan, *Member, IEEE*, and Hong Shen

**Abstract**—X. Liang systematically investigated orthogonal designs with maximal rates, gave the maximal rates of complex orthogonal designs and a concrete construction procedure for complex orthogonal designs with the maximal rates. He also posed an open problem on the minimal decoding delays of complex orthogonal designs with maximal rates, and proved that the problem is correct for less than or equal to six transmit antennas. In this correspondence, we give a counterexample for the open problem for  $\tau = 8$  and prove that the minimal delay for complex orthogonal designs with eight columns is 56. Hence, we give a negative answer for the open problem.

**Index Terms**—Complex orthogonal designs, decoding delays, full diversity, maximal rates, space-time block codes.

### I. INTRODUCTION

Recently, space-time codes have been extensively investigated for wireless communication systems with multiple transmit and receive antennas. Alamouti [1] proposed a remarkable transmission scheme using two transmit antennas, which has linear maximum-likelihood (ML) decoding complexity and full diversity. Subsequently, Tarokh, Jafarkhani, and Calderbank [9] generalized Alamouti's idea to the general case by orthogonal designs, i.e., space-time codes from orthogonal designs, and provided a systematic method to construct real orthogonal designs with code rate 1 and complex orthogonal designs with code rate  $1/2$ . It was proved in [8] and [9] that the code rate of real or complex orthogonal designs is not larger than 1. Hence, what are the maximal rates for complex orthogonal designs is an open problem. Lately, an upper bound of the maximal rate for space-time codes from generalized complex orthogonal designs was given by Wang and Xia in [11] by use of elegant matrix analysis. However, we do not know if the upper bound in [11] can be achieved for more than four transmit antennas. At almost the same time, Liang [3] systematically and smartly investigated the maximal rates of space-time codes from complex orthogonal designs: he not only gave the maximal rates of complex orthogonal designs for any number of transmit antennas, but also presented a concrete construction procedure for complex orthogonal designs with the maximal rates. Furthermore, Liang discussed the minimal decoding delays of complex orthogonal designs with the maximal rates. He proved that the complex orthogonal designs with the maximal rates obtained from his construction procedure have the minimal decoding delays for fewer than or equal to six transmit antennas, and posed an open problem for the minimal decoding delays.

In the correspondence, we give a counterexample for the open problem in [3], thus giving a negative answer to the open problem. In Section II, we introduce some preliminaries on orthogonal designs. A

Manuscript received February 26, 2004; revised June 1, 2004. This work was supported by the National Science Foundation of China under Grants 60003007 and 60472038 as well as by the Japan Society for Promotion of Science (JSPS) under Research Grant 14380139.

H. Kan is with the Graduate School and Information Science, Japan Advanced Institute of Science and Technology, 1-1, Asahidai, Tatsunokuchi, Ishikawa, 923-1292, Japan. He is also with the Department of Computer Science and Engineering, Fudan University, Shanghai, China (e-mail: haibin@jaist.ac.jp).

H. Shen is with Graduate School and Information Science, Japan Advanced Institute of Science and Technology, 1-1, Asahidai, Tatsunokuchi, Ishikawa, 923-1292, Japan (e-mail: shen@jaist.ac.jp).

Communicated by Ø. Ytrechus, Associate Editor for Coding Techniques.  
Digital Object Identifier 10.1109/TIT.2004.839544